IN THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,

Plaintiffs,

4:15CR3078

VS.

CLIFTON HUDSON.

Defendant.

FINDINGS, RECCOMENDATION AND ORDER

The defendant moved to suppress subscriber and cell-site information obtained by the government through the execution of several search warrants issued by District and County Court judges in Buffalo County, Nebraska (<u>Filing No. 61; Filing No. 62 at CM/ECF pp. 9–11</u>). For the reasons discussed below, the motion to suppress should be denied.

BACKGROUND

On October 17, 2014, the Kearney Eaton Employee's Credit Union (KEECU) located at 2600 East Highway 30 in Kearney, Nebraska was robbed by two unknown African American males. The same individuals had been recorded on surveillance video near the credit union on October 16 between the hours of 11:00 am and 1:00 pm and investigating officers believed the individuals had been scouting the area at that time. Based on this video, the City of Kearney Police Department ("KPD") concluded it was likely these individuals had placed cell phone calls around this time and the time of the robbery. On October 24, 2014, the KPD submitted two identical search warrant applications to Buffalo County District Judge William T. Wright The applications sought production of

[a]ll available toll records to include call details for incoming and outgoing calls, cell site and cell site towers nearest to 2600 E. Highway 30, Kearney, Buffalo County Nebraska for all calls made between 11:00 A.M. and 2:00 P.M. on October 16, 2014 and between 8:00 A.M. and 11:00 A.M. on October 17, 2014.

(Filing No. 73-1 at CM/ECF p. 1; Filing No. 73-2 at CM/ECF p. 1). The warrants were directed to two cell phone service providers; Cellco Partnership d/b/a Verizon Wireless and U.S. Cellular. Judge Wright granted both warrant applications and issued the requested warrants.

Based upon further investigation and findings, on December 3, 2014, KPD sought a search warrant for U.S. Cellular phone records pertaining to Hudson's phone number. Specifically they sought

[a]ny and all cellular telephone records for telephone number 402-637-4457 to include but not limited to, billing information, as well as dates, times, content, and telephone numbers of incoming and outgoing text messages and incoming and outgoing of phone calls, also information concerning IP addresses that text messages may have been sent from or received from, from 09/01/2014 to 10/31/2014.

(<u>Filing No. 73-3 at CM/ECF p. 1</u>). Buffalo County Court Judge Rademacher found probable cause to grant the warrant applications, and issued the requested warrants as written.

On December 11, 2014, KPD sought a warrant from Sprint for "any and all cell tower information for telephone number 402-637-4457 from 09/01/2014 to 10/31/2014." (Filing No. 73-4 at CM/ECF p. 1). Buffalo County Court Judge Jorgensen granted the warrant.

On January 9, 2015, KPD sought a warrant for U.S. Cellular phone records regarding Hudson's second phone number. They requested

[a]ny and all cellular telephone records for the telephone number 402-637-8654 to include but not limited to, billing information, dates and times of calls received or dialed as well as dates and times of all text messages received and sent and the content of both received and sent text messages, also information concerning IP addresses that text messages may have been sent from or received from, for the dates of 09/01/2014 to 10/31/2014, also all cell tower information pertaining to this number from this time frame.

(Filing No. 73-6 at CM/ECF p. 1). Judge Jorgensen granted the warrant.

On February 3, 2015, KPD sought a warrant from Cellco Partnership d/b/a Verizon Wireless for

[a]ny and all cellular telephone records for telephone number 402-637-4457 to include but not limited to, subscriber information, as well as dates, times, content, and telephone numbers of incoming and outgoing text messages and incoming and outgoing of phone calls, also information concerning IP addresses that text messages may have been sent from or received from, as well as cell tower information from 09/01/2014 to 10/31/2014.

(<u>Filing No. 73-5 at CM/ECF p. 1</u>). Judge Jorgensen granted the warrant.

Hudson now seeks to suppress any information gathered from the above described warrants. He argues that the warrants were issued in violation of his Fourth Amendment rights.

ANALYSIS

The Fourth Amendment guarantees citizens the right to be free from unreasonable searches and seizures. U.S. Const. amend. IV. For the Fourth Amendment to attach, the defendant must have a reasonable expectation of privacy in the area searched or the items seized. Rakas v. Illinois, 439 U.S. 128, 143 (1978); Katz v. United States, 389 U.S. 347, 361 (1967). A defendant who challenges a search or seizure bears the burden of proving he has a reasonable expectation of privacy in searched or seized items. Rawlings v. Kentucky, 448 U.S. 98, 104–05 (1980). Only where the Fourth Amendment has been violated should a party "benefit from the [exclusionary] rule's protection." Rakas, 439 U.S. at 134.

"A person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." <u>United States v. Miller, 525 U.S. 435, 442–44 (1976)</u>; <u>Smith v. Maryland, 442 U.S. 735, 743–44 (1979)</u>. "[W]hen an individual reveals private information to another, he assumes the risk that this confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information." <u>United States v. Jacobsen, 466 U.S. 109, 117 (1984)</u>. Under the third-

party doctrine, courts have consistently held that individuals lack a reasonable expectation of privacy in basic telephone records. See Smith, 442 U.S. at 745 (holding defendant did not have a reasonable expectation of privacy in the phone numbers dialed); United States v. Clenney, 631 F.3d 658, 666 (4th Cir. 2011) (holding no privacy interest in basic subscriber information); United States v. Phibbs, 999 F.2d 1053, 1077 (6th Cir. 1993) (holding no privacy interest in telephone records).

1. Non-content Information Requested

More recently, with the advance of technology, courts have concluded "that defendants have no reasonable expectation of privacy in historical cell-site data." United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015)(en banc); United States v. Guerrero, 768 F.3d 351, 359–60 (5th Cir. 2014); United States v. Jones, 908 F. Supp. 2d 203, 211 (D.D.C. 2012); United States v. Ledbetter, 2015 WL 7758930, * 12–13 (S.D. Ohio Dec. 2, 2015). Courts analyzing this question have concluded the third-party doctrine applied when examining requests for historical cell-site information because the defendants (1) voluntarily conveyed their information to the cell phone company; and (2) the companies maintain that information in the ordinary course of business. Jones, 908 F. Supp. 2d at 211. In its holding, the Fifth Circuit reasoned, "cell phone users voluntarily convey information to their service providers . . . and '[they] understand that their service providers record their location information when they use their phones." Guerrero, 768 F.3d at 358 (citations omitted).

¹ Cellular service providers utilize a system of towers to receive and transmit signals from cell phones. When a cell phone user places or receives a call, the cell phone sends a signal that is picked up by the nearest tower. Cellular service providers generate and maintain records of a cell phone tower's activities in the regular course of business: This information is referred to as historical cell-site information. Historical cell-site information includes the time a call or text message is made or received; the telephone numbers involved in the communication; the cell tower; and the duration of the call. Jones, 908 F. Supp. 2d at 207–08.

² For an extensive list of cases holding that there is no reasonable expectation of privacy in historical cell-site records, see <u>Jones</u>, 908 F. Supp. 2d at 211 n.9.

But other courts that have held a cellphone user has a reasonable expectation of privacy in historical cell-site location information. <u>United States v. Graham, 796 F.3d 332</u> (4th Cir. 2015); In re Tel. Info. Needed for a Crim Investigation, 2015 WL 4594558 (N.D. Cal. July 29, 2015); Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2013). Typically, in these cases, search warrants or orders are sought by the government to trace an individual's movement -- similar to requesting GPS monitoring or tracking. <u>See Id.</u> Refusing to rely on the third-party doctrine, these courts reason that location information may be sent to a cell tower even while the user's phone is idle and is not voluntarily shared by the user. <u>Graham, 796 F.3d at 357</u> ("Applying the third-party doctrine in this context would simply permit the government to convert an individual's cellphone into a tracking device by examining the massive bank of location information retained by [his] service provider.")

Hudson states he has standing to challenge the government's acquisition of both the information directly related to his cell phones records and the cell-site information. The October 24th warrants sought call information for any calls that used cell towers located near the KEECU. The December 11th warrant sought cell tower information for one of Hudson's telephone numbers for the months concerning the robbery. Both of these warrants sought only historical cell-site information that defendant voluntarily shared with his third-party cell phone service provider.

The remaining three warrants, dated December 3rd, January 9th, and February 3rd, sought various non-content records associated with Hudson's two cell phones: billing/subscriber information; dates and times of text messages and phone calls; the telephone numbers or IP addresses involved; and cell tower information associated with the phone number. Like historical cell-site information, subscriber information, which includes not only a user's name and billing information, but also his billing records with the phone numbers and IP addresses dialed and received, is information shared with and collected by the user's cell phone carrier. See Ledbetter, 2015 WL 7758930 at *13; Huon v. Mudge, 597 F. App'x 868, 875 (7th Cir. 2015); United States v. Davis, 785 F.3d 498, 511 (11th Cir.

<u>2015</u>) (en banc). The court notes some of this information has never been protected, and this does not change simply because the phone records arise from use of a cell phone rather than a landline. <u>See Smith</u>, <u>442 U.S. at 745</u> (no reasonable expectation of privacy in the phone numbers dialed).

Hudson does not argue that the KPD sought Hudson's cell-site information to track Hudson's movements and the warrants do not indicate location monitoring information was obtained. Instead, the challenged warrants requested other basic cell-site and subscriber information. For this reason, Hudson's reliance on cases addressing historical and prospective location information is misplaced.

Hudson argues the Supreme Court's recent holding in <u>Riley v. California</u>, extends to his cell phone records. <u>134 S. Ct. 2473 (2014)</u>. In <u>Riley</u>, the Court addressed whether a police officer may search a suspect's cell phone incident to a lawful arrest. In making its decision, the Court indisputably held that an individual has a reasonable expectation of privacy in the digital contents of his phone. In its reasoning, the Court emphasized:

[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it contains a broad array of private information never found in a home in any form[.]

<u>Id. at 2491</u>. But basic telephone records and historical cell-site information are not 'sensitive records' that a person may keep on a cell phone or in a home. Cell-site information is not private information; it is information gathered and documented by a third party in the regular course of business. Accordingly, Defendant's reliance on <u>Riley</u> is misplaced. <u>See Guerrero</u>, 768 F.3d at 359–60; <u>Ledbetter</u>, 2015 WL 7758930 at *14.

2. Content Information Requested

The December 3rd, January 9th, and February 3rd warrants also sought the content of Hudson's text messages and calls. The issue of whether an individual has a reasonable

expectation of privacy in the content of his electronic communications is in debate. Several courts, including the United States Supreme Court, have deferred ruling on this issue. City of Ontario v. Quon, 560 U.S. 746, 760 (2010); United States v. Grooms, 566 Fed. Appx. 485, 490 (6th Cir. 2014). A few courts have determined that an individual has a reasonable expectation of privacy in the content of his text messages and calls. See, e.g., Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, (9th Cir. 2008) (rev'd on other grounds) (users have a reasonable expectation of privacy in the content of their text messages); United States v. Finley, 477 F.3d 250, 259 (5th Cir. 2007).

While Hudson *may* have standing to challenge any seizure of the cell phone content gathered through the warrants, the court will not rule on this issue in the current motion. It is unclear from the record whether any content was gathered or is at issue for this motion. The Government's brief repeatedly indicates contents of communications were not requested. (See Filing No. 89 at CM/ECF pp. 5, 7, 18), and Defendant's argues to exclude subscriber and cell-site information, not the content of text messages or calls. (See Filing No. 62 at CM/ECF pp. 9–11). Nevertheless, the December 3rd, January 9th, and February 3rd warrant applications unambiguously requested the content of text messages and calls. (See Filing Nos. 73-3, 73-5, & 73-6). Since neither party mentions that cell phone or text message content was obtained as a result of executing the warrants at issue, the court is left to wonder if an issue even exists regarding this information. This court should "avoid deciding constitutional matters in a vacuum," and will not enter into the debate without evidence that such content exists and that it was gathered in violation of Defendant's constitutional rights. Grooms, 566 Fed. Appx. at 490.

Hudson has failed to prove he has a reasonable expectation of privacy in the cell phone records and cell site information obtained through the challenged warrants. As such, Defendant's request for a <u>Frank's</u> Hearing is denied.

IT THEREFORE HEREBY IS RECOMMENDED to the Honorable Richard G. Kopf, Senior United States District Judge, pursuant to <u>28 U.S.C.</u> § <u>636(b)</u>, that the motion to suppress filed by the defendant (<u>Filing No. 28</u>) be denied in its entirety.

The defendant is notified that failing to file an objection to this recommendation as provided in the local rules of this court may be held to be a waiver of any right to appeal the court's adoption of the recommendation.

IT IS ORDERED that the jury trial of this case is set to commence before Richard G. Kopf, Senior United States District Judge, in Courtroom 1, United States Courthouse, Lincoln, Nebraska, at 9:00 a.m. on March 21, 2016 or as soon thereafter as the case may be called, for a duration of five (5) trial days. Jury selection will be held at the commencement of trial.

Dated this 19th day of February, 2016

BY THE COURT:

s/ Cheryl R. Zwart
United States Magistrate Judge

^{*}This opinion may contain hyperlinks to other documents or Web sites. The U.S. District Court for the District of Nebraska does not endorse, recommend, approve, or guarantee any third parties or the services or products they provide on their Web sites. Likewise, the court has no agreements with any of these third parties or their Web sites. The court accepts no responsibility for the availability or functionality of any hyperlink. Thus, the fact that a hyperlink ceases to work or directs the user to some other site does not affect the opinion of the court.